Face
Facultad de Ciencias Económicas y Empresariales

ISSN Impreso: 1794-9920
ISSN Electrónico: 2500-9338
Volumen 18-N°2
Año 2018
Págs. 78 - 96

# EL NUEVO REGLAMENTO GENERAL EUROPEO DE PROTECCIÓN DE DATOS PRESENTE Y FUTURO

Verónica Juliana Caicedo Buitrago *
Enlace ORCID: https://orcid.org/0000-0002-7887-6323

Fecha de Recepción: Septiembre 20 de 2018
Fecha de Aprobación: Diciembre 22 de 2018

## Resumen:

El Derecho de Protección de Datos de carácter personal de las personas físicas es una cuestión que se viene tratando desde hace ya varios años, es más, nos podemos remontar a la Declaración Universal de Derechos Humanos de 1948, la cual, ya mencionaba la protección de datos, sin embargo, es hasta 1981 cuando en Europa se tiene el primer antecedente legislativo sobre dicha protección. Posteriormente, se promulgó una Directiva en el año 1995. No obstante, este tema no había sido tomado en serio por los países de la Unión Europea, aunque la Directiva fue traspuesta en los Estados miembro. Pasados algunos años, producto del avance de la sociedad y las nuevas tecnologías se hizo necesario regularlo, a través de un mecanismo de obligatorio y directo cumplimiento para todos, es así, como nace el Reglamenteo General Europeo de Protección de Datos cuyo obligatorio y directo cumplimiento se exige desde el 25 de mayo de 2018. En la actualidad, los Estados miembro debían estar totalmente adaptados, pero no ha sido así, aún quedan cuestiones por resolver, obligados por adaptarse y normas por legislarse.

**Palabras clave:** Reglamento Europeo de Protección de Datos; Protección de Datos, Derecho Fundamental; medidas; Unión Europea.

* Doctora en Derecho, Máster en Derecho Deportivo, Máster en Derecho de Familia y Sistemas Hereditarios. Abogada del Ilustre Colegio de Abogados de Madrid, Abogada Inscrita en el Consejo Superior de la Judicatura de Colombia, Profesora en la Universidad Alfonso X el Sabio de Madrid-España. Contacto: vbuitcai@myuax.com; v.caicedo.buitrago@gmail.com

**THE NEW EUROPEAN GENERAL DATA PROTECTION REGULATION. PRESENT AND FUTURE.**

**Abstract:**

The Right to Protection of Personal Data of Individuals is an issue that has been discussed for several years, is more, we can return to the Universal Declaration of Human Rights of 1948, which, mentioned data protection, however, is until 1981 when in Europe you have the first legislative precedent on this issue. Subsequently, a Directive was promulgated in 1995. However, this issue had not been taken seriously by the countries of the European Union, although the Directive was transposed in the Member States. After a few years as a result of the advancement of society and new technologies, it became necessary to regulate it, through a mechanism of mandatory and direct compliance for all, that is how the General European Regulation of Data Protection was born, whose obligatory compliance is demanded from the May 25, 2018. At present, the member States must be fully adapted, but this has not been the case, there there are still issues to be solved, bound to adapt and law to be legislated.

**Keywords:** European Data Protection Regulation; Data Protection; Fundamental right; actions; European Union.

## O NOVO REGULAMENTO EUROPEU GERAL DE PROTEÇÃO DE DADOS. PRESENTE E FUTURO

**Resumo:**

O Direito à Proteção de Dados Pessoais de Indivíduos é uma questão que vem sendo discutida há vários anos, é mais, podemos retornar à Declaração Universal dos Direitos Humanos de 1948, que, mencionada proteção de dados, é até 1981 quando na Europa você tem o primeiro precedente legislativo sobre esta questão. Subsequentemente, foi promulgada uma directiva em 1995. No entanto, esta questão não foi levada a sério pelos países da União Europeia, embora a directiva tenha sido transposta nos Estados-Membros. Após alguns anos, como resultado do avanço da sociedade e das novas tecnologias, tornou-se necessário regulá-la, através de um mecanismo de cumprimento obrigatório e direto para todos, e assim nasceu o Regulamento Europeu Geral de Proteção de Dados, cuja obrigatoriedade de cumprimento é exigido a partir de 25 de maio de 2018. Actualmente, os estados membros devem ser totalmente adaptados, mas isto não tem sido o caso, há ainda questões a serem resolvidas, obrigadas a adaptar e a lei a ser legislada.

**Palavras-chave:** Regulamento Europeu de Proteção de Dados; Proteção de dados; Direito fundamental; ações; União Européia.

ISSN: 1794-9920 Julio – Diciembre de 2018
Volumen 18 Número 2, Año 2018 Págs. 78 - 96

## 1. INTRODUCCIÓN:

La protección de los datos de las personas físicas en Europa viene siendo una cuestión permanente y constante desde hace varias decadas, sobre todo cuando en los años 90`s y producto del modelo de integración llamado Unión Europea (en adelante UE), se le dio paso a la libre circulación de las personas dentro del territorio de la misma y por ende la libre circulación de los datos de éstas. Por esta razón y cumpliendo con las necesidades que demanda la sociedad, los entes administrativos de la Unión Europea junto con los Estados miembro han regulado este asunto. Aunque, sigue habiendo un gran desconocimiento sobre el tema y a la vez una desidia por parte de muchos ciudadanos tanto europeos como no europeos a quienes les afectan estos cambios, lo cierto es que esta cuestión cada vez se hace más importante.

En materia de protección de datos, el último gran acontecimiento ocurre el 25 de mayo de 2018, fecha en la que Europa empezó a experimentar grandes cambios en lo referente a este tema, ya que fue esta la fecha que estipuló el Parlamento Europeo para que entrara en vigor el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)[1], (en adelante, RGPD). Pues bien, como no podía ser otra manera y como expondré en las próximas páginas, muy pocos europeos se prepararon y adaptaron a esta nueva normativa antes de que fuese de directa y obligatoria aplicación. Por ello, Europa se ha visto retada por un sinfin de datos corriendo por todos sus rincones, buscando refugio en uno y otro lugar, acompañada de un incumplimiento normativo por parte de aquellos que ni aplicando su mayor velocidad, han logrado llegar a la mencionada fecha con los deberes hechos y los ajustes realizados.

Ahora bien, con la finalidad de poder explicar qué es lo que ha ocurrido, y hacía dónde va Europa en materia de protección de datos, iniciaremos haciendo una breve reflexión sobre los, datos de las personas físicas, para luego hacer memoria y contar a través de la historia, qué se ha dicho sobre la protección de datos en Europa, pasando por las dinstintas menciones y regulaciones hasta llegar al RGPD; seguidamente explicaremos la ruta y las mediadas que hay que tomar, para adpatarse a esta nueva normativa; finalmente concluiremos expresando, a nuestro modo de ver, cuál es el futuro más inmediato de la implementación y aplicación del meritado reglamento.

[1] https://www.boe.es/doue/2016/119/L00001-00088.pdf Visitada 20/10/2018 a las 19:00

Dicho lo anterior, para empezar, me gustaría que el lector hiciera un ejercicio: Por un momento piense ¿qué entiende por dato personal? Pues bien, le surgirán distintas y variopintas respuestas. Una palabra, un nombre, una información concreta, etcétera. Todo esto está muy bien pensado, ya que para la legislación europea un dato personal es: "[...] toda informaciíon sobre una persona física identificada o identificable […]"[2].

Pensemos, por ejemplo, en nuestro nombre: María, Pedro, Andrés, Laura quizá. Y preguntémonos ¿a quién le puede interesar este dato? Pues podríamos pensar, bueno yo no le importo a nadie o los más optimistas dirán, no le importo a nadie más que a mi familia o a mis amigos. Pues quiero comunicarles que cada uno de los que están leyendo estas letras son sumamente importantes, además tal y como van las nuevas técnologias, hoy en día, cada vez ustedes que están leyéndome son más importantes. También, sé que muchos pretendemos ser discretos, pero quiero dejarles algo claro: siempre somos importantes para alguien. De hecho, permítanme contarles o recordarles una anécdota, hace unos años rodaba en Colombia un correo electrónico que decía: "No se preocupe si siente que nadie se acuerda de usted, nosotros siempre nos acordamos. Atentamente: Dirección de Aduanas e Impuestos Nacionales (DIAN). Más alla del ejemplo, es verdad, que somos importantes para todas las personas, entidades y empresas que quieren saber de nosotros, bien porque tienen alguna relación con nosotros; y aunque creamos que son pocos insisto, nuestros datos interesan a muchos, bien porque quieran llegar a tener alguna relación con nosotros, en fin, nuestros datos interesan a quien por algún motivo o razón quiere saber de nosotros.

Pues bien, hecho el ejercicio me place comentarles que, producto del interés de muchos por los datos de otros nace el Reglamento Europeo de Protección de Datos.

## 2. ANTECEDENTES:

Como antecedentes precursores de la protección de datos personales encontramos la Declaración Universal de los Derechos Humanos de 1948[3] que en el artículo 12 menciona que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o correspondencia, ni ataques a su honra o reputación. Toda persona tiene derecho a la protección de la Ley contra

[2] Artículo 4.1 Reglamento General Europeo de Protección de Datos.

[3] https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf Visitada 20/10/2018 a las 18:40.

tales injerencias o ataques". A su vez, encontramos tanto la Carta de los Derechos Fundamentales de la Unión Europea[4] como el Tratado de Funcionamiento de la Unión Europea[5], instrumentos que en los artículos 8 y 16.1 respectivamente mencionan la protección de datos de las personas físicas como un derecho fundamental. También, lo incluye el Convenio Europeo para la protección de los Derechos Humanos y Libertades fundamentales del Consejo de Europa[6]. Sin embargo, hemos de hacer la salvedad de que estos instrumentos simplemente mencionan la protección de datos y su carácter de especial protección, pero no lo regulan, ni entran en detalle sobre el tema.

Tras lo anteriormente dicho, encontramos que la primera legislación de la que tenemos conocimiento sobre esta cuestión aparece el 28 de enero de 1981, a través del Convenio 108 del Consejo de Europa[7] que fue el que vino a matizar y a regular lo que ya se había mencionado. Ahora bien, por causa de la evolución de la sociedad y con la apertura hacia la libre circulación de las personas por el territorio de la UE a principios de los 90`s, también empezaron a circular libremente los datos. Por esta razón y como respuesta a la evolución social, la UE se vio obligada en el año 1995 a promulgar la Directiva[8] 95/46/CE[9] relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y libre circulación de los mismos. Pues bien, esta Directiva fue extrapolada a todos los Estados miembro de la UE, por ejemplo, en España se promulgó la Ley Orgánica 5/1995, de 13 de diciembre, de Protección de Datos de Carácter Personal[10], (en adelante LOPD). No obstante, y no contenta con lo conseguido, la sociedad siempre más adelante que el Derecho y exigiéndole cada vez más, además acompañada de las nuevas tecnologías generó el estudio de la protección de datos como un tema fundamental dentro de la legislación europea, ya que, si bien es cierto, la Directiva del 95 fue extrapolada a los Estados miembro, la misma no se cumplía a total cabalidad, es más, aún con el nuevo RGPD, quienes están obligados a cumplirlo todavía confunden los conceptos y medidas derivadas de la Directiva y las derivadas del nuevo Reglamento.

Entonces, con la finalidad de reestructurar lo que ya se había legislado sobre el tema de la protección de los datos y añadir cuestiones nuevas, se iniciaron varios estudios por parte de los órganos de la UE, estudios que abrieron paso al nuevo RGPD, que fue aprobado por el pleno del Parlamento Europeo el 14 de abril de 2016 y publicado en el Diario Oficial de la Unión Europea, el 4 de mayo del mismo año[11]. Dicho instrumento, entró en vigor el 25 de mayo de 2016, pero la UE preocupada por sus miembros y entendiendo que la adaptación al mismo podía tardar cierto tiempo, decidió en pro de éstos conceder el plazo de 2 años para que fuera de aplicación obligatoria y directa a todos los Estados miembro, esto es, hasta el 25 de mayo de 2018, plazo que verdaderamente era razonable para generar la adaptación, sin embargo, en octubre 2018, esto es cuatro meses después de que el RGPD empezara a ser de obligatorio cumplimiento para todos los Estados miembro, todavía hay obligados a cumplirlo que no se terminan de adecuar. Hemos de decir que, el RGPD es un reglamento bastante general que se ha dedicado a marcar las pautas sobre la protección de datos, quizá le podríamos llamar Reglamento "marco", toda vez que, deja varias cuestiones para que cada unos de los Estados miembro las reglamente como a bien lo tengan, con lo cual, es necesario matizar las ideas dentro de cada Estado.

### 1. ¿Qué ocurre en la actualidad?

Actualmente, Europa está en proceso de adaptación, como no podía ser de otra manera, los europeos han esperado hasta el último momento para iniciar las labores de adecuación, es más, algunos aún no se han adecuado, escasamente están pensando en hacerlo y eso que el Reglamento ya lleva casi un año en vigor y trae consigo reguladas sanciones por incumplimiento de hasta VEINTE MILLONES DE EUROS (20.000.000 €). Entonces, cabe preguntarnos ¿por qué está ocurriendo esto? Pues bien, la única respuesta posible es que nadie se había tomado en serio la protección de los datos, lo que no sabemos concretamente, es cuál es la razón, tal vez, falta de tiempo,

[4] http://www.europarl.europa.eu/charter/pdf/text_es.pdf Visitada 20/10/2018 a las 18:42

[5] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12012E%2FTXT Visitada 20/10/2018 a las 18:45

[6] https://www.echr.coe.int/Documents/Convention_SPA.pdf Visitada 20/10/2018 Visitada 20/10/2018 a las 18:46

[7] http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=filename%3DCONVENIO%25201 08.pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1202800216772&ssbinary=true Visitada 20/10/2018 a las 18:47

[8] La legislación de la Unión Europea se compone de Reglamentos, Directivas y Decisiones, nos centraremos en los dos primeros, simplemente para hacer una aclaración que nos puede llevar a entender cómo funcionan ambos instrumentos. La principal diferencia y la que quiero resaltar en el marco de este escrito es que el reglamento se transpone directamente, esto es, cuando se promulga un nuevo reglamento, el mismo es de obligatorio cumplimiento para todos los Estados miembro de forma directa y automática, es decir, pasan a ser parte de la legislación de cada uno de los Estados miembro. A contrario sensu, no funciona igual con la Directiva, ya que este instrumento debe ser traspuesto a la legislación de los distintos Estados. ¿Cómo se hace? A través de los procedimientos legislativos de cada uno de los Estados miembro.

[9] https://www.boe.es/doue/2016/119/L00089-00131.pdf Visitada 20/10/2018 a las 18:50

[10] https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750 Visitada 20/10/2018 a las 18:51

[11] https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1549367809314&uri=CELEX:32016R0679 Visitada 22/10/2018 a las 18:00

ISSN: 1794-9920 Julio – Diciembre de 2018
Volumen 18 Número 2, Año 2018 Págs. 78 - 96

apatía, poca importancia. Pero, podemos llegar a concluir simplemente por el hecho de observar lo que ocurre, que fundamentalmente es una cuestión de ignorancia.

Lo que está pasando es que los Estados miembro vieron salir la Directiva en el 95 y al ser Directiva, como ocurre con tantas otras cosas dentro de este modelo de integración llamado UE dijeron: regulamos la Directiva cumplimos y ya está. Pero, realmente dentro de los Estados las personas no se implicaron mucho en lo referente a la aplicación de la misma, de hecho, centrándonos en el caso español, que podemos decir que, no es distinto de muchos otros, se promulgó la LOPD, pero prácticamente nadie tenía conocimiento de las obligaciones que la misma exige, se mencionaba, pero no se aplicaba, tanto es así insisto, que ha salido el nuevo Reglamento y hay ciudadanos que confunden lo que exige la Ley con lo que exige el Reglamento.

Además, desde este epígrafe insisto y advierto para los posteriores que el Reglamento es muy general, es como mencioné, un Reglamento "marco" que deja al arbitrio de los Estados miembro la decisión sobre la forma de aplicación y reglamentación de varias cuestiones, con lo cual, los Estados no sólo deben limitarse a la aplicación del meritado instrumento, si no que también, deben empezar a reglamentar lo que a bien tienen para cada una de sus naciones.

## 2. ¿Qué exige el reglamento?

En este punto, hemos de distinguir tres aspectos, el primero ¿qué se protege?; el segundo ¿a quién se protege? Y; el tercero ¿a quién se debe proteger? Pues bien, lo que se protege son los datos personales de las personas físicas, esto es, los datos de carácter personal definidos en el RGPD como: "[…] cualquier información referente a personas físicas identificadas o identificables, pudiendo ser identificable toda persona cuya identidad pueda determinarse mediante un identificador".

También, existe una categoría de datos especialmente protegidos que son aquellos referentes a datos de salud, datos que puedan revelar el origen étnico o racial, opiniones políticas, convicciones religiosas o fisiológicas, o afiliación sindical, así como el tratamiento de los datos genéticos, biométricos y, datos sobre la vida sexual u orientación sexual.

Ahora bien y como segundo tema, ¿a quién se protege? De acuerdo al RGPD, se protege a las personas físicas sin importar su nacionalidad, ni el lugar de residencia mientras mantengan alguna relación con alguna entidad que preste sus servicios en Unión Europea. También se protegen los datos seudonimizados que son aquellos que cabe atribuir a una persona física mediante la utilización de información adicional, ya que esto se consideran información sobre una persona física identificable[12].

No obstante, me gustaría hacer alusión especial a ¿qué ocurre con los datos de los menores? El RGPD regula esta cuestión en el artículo 8, así nos dice que, como norma general, se entienden menores, las personas físicas menores de 16 años. Sin embargo, deja abierta la posibilidad para establecer la minoría de edad a los Estados miembro, de acuerdo a su legislación, siempre y cuando ésta no sea inferior a 13 años. En el caso español, según el artículo 13.1 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[13], a efectos de la protección de datos se entienden menores de edad aquellas personas físicas que no hayan cumplido 14 años. Además, hemos de tener en cuenta que el ofrecimiento directo de servicios por internet a menores requiere del consentimiento de su representante legal y en todo caso, la información sobre tratamiento de datos dirigida a los menores se debe realizar en un lenguaje claro y sencillo para los mismos.

Finalmente, consideramos importante mencionar en qué casos no se aplica el RGPD. Esta protección no se aplica a los datos personales de personas fallecidas, en estos casos los Estados miembro son los competentes para establecer las normas relativas al tratamiento de estos datos. De otro lado, pero en consonancia con el tema, en el RGPD tampoco se regula el tratamiento de datos de personas jurídicas. Finalmente, también hemos de hacer la salvedad sobre la aplicación del reglamento a datos de personas físicas, que se encuentren en el curso de una actividad exclusivamente personal o doméstica[14] y, por tanto, sin conexión alguna con una actividad profesional o comercial, en estos casos no se aplica el tratamiento de datos de carácter personal. Sin embargo, el RGPD si se aplica a quienes tratan los datos personales relacionados con las actividades personales o domésticas, por ejemplo, pensemos en qué una ama de casa tiene una red social, caso en el cual, sus datos serán tratados por la empresa que le presta el servicio.

[12] Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.

[13] https://www.boe.es/buscar/act.php?id=BOE-A-2008-979 Visitada el 11/11/2018 a las 12:12

[14] Dentro de las actividades personales o domésticas cabe incluir: la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y, la actividad en línea realizada en el contexto de las citadas actividades.

Seguidamente y como tercer tema, ¿Quién o quienes deben proteger? Los obligados a proteger los datos son: Las Administraciones Públicas; las empresas u otras entidades que sean responsables del tratamiento de datos, esto es, todos aquellos a quienes las personas físicas han facilitado sus datos de carácter personal.

En lo referente a las empresas, hemos de decir que no todas las empresas están obligadas, pero sí, la gran mayoría, ya que deben proteger los datos de las personas físicas todas aquellas empresas o profesionales autónomos establecidos en la UE, independiente de si el tratamiento efectivo tiene lugar o no en el territorio de la UE. También lo deben hacer, todas aquellas empresas que aún sin residir en la UE se dediquen a ofrecer bienes y/o servicios independientemente de si los mismos son de pago o no, y también aquellas que por su labor puedan tener control sobre el comportamiento de las personas dentro de la UE.

## 3. ¿Cómo nos adaptamos al RGPD?

Para adaptarnos al RGPD es preciso realizar una secuencia de pasos que los hemos clasificado en dos categorías, pasos externos y pasos internos, conceptualizando los pasos externos como aquellos que son públicos para los usuarios y los pasos internos como aquellos que son conocidos única y exclusivamente por quien trata los datos. Entonces, en los dos siguientes epígrafes explicaremos los mencionados pasos, iniciando por los internos y finalizando por los externos.

### 2.1. Pasos Internos

Dentro de este apartado estudiaremos cada uno de los pasos internos que deben realizar quienes tratan datos, para adaptarse al RGPD. Los definimos como pasos internos porque se constituyen como la secuencia de actos que debe realizar la empresa, el autónomo, en fin, quien trata los datos para adecuarse al RGPD. Además, los mismos serán conocidos sólo por quien o quienes sean parte integrante del tratante de datos, esto significa que todo aquél que no lo sea incluidos los usuarios en principio no los conocerán, y no porque sean secretos o exista la obligación de guardarlos, simplemente, porque a los usuarios no les tiene porque interesar, éstos simplemente lo que desean es que sus datos sean protegidos independientemente de cómo se haga. Ahora bien, estos pasos se deben realizar, ya que son los que permiten que se puedan proteger adecuadamente los datos de las personas, por esta razón se hacen necesarios y forman parte de la cadena de protección de datos.

#### 2.1.1 Designar un Delegado de Protección de Datos

El primero de los pasos internos es designar un Delegado de Protección de Datos (en adelante DPO, por sus siglas en inglés *Data Protection Officer*), hemos de aclarar que este paso lo tendrán que completar obligatoriamente sólo quienes indique el Reglamento, sin embargo, también hemos de hacer la siguiente salvedad, cualquier empresa que lo estime conveniente puede designar un DPO, de hecho, se recomienda nombrar uno. ¿Cuáles son los casos obligatorios? Estos vienen recogidos en el artículo 37 RGPD y principalmente son tres casos, el primero, que el tratamiento lo lleve a cabo una autoridad u organismo público; el segundo, que las actividades principales del responsable o encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala. En este punto, cuando el RGPD se refiere a actividad principal, lo que nos quiere decir es que, el tratamiento de determinados datos es el objetivo principal de la empresa, por ejemplo, una empresa dedicada a prestar servicios de red social que maneje perfiles con los datos de las personas físicas, o cuando el tratamiento sea intrínseco a la función, por ejemplo, una clínica privada donde no es posible acudir sin conocer los datos de los pacientes. Sin embargo, hay otros datos que, aunque requieren de protección se entienden a efectos del nombramiento del DPO como auxiliares, volviendo al ejemplo de la clínica privada, diremos que el tratamiento intrínseco son los datos de los pacientes, mientras que los datos que se recogen con la finalidad de pagar la nómina a sus empleados, se entienden como datos de actividad auxiliar.

El tercer caso que se regula se presenta cuando las actividades principales del responsable o el encargado consistan en el tratamiento a gran escala de las categorías especiales de datos o datos personales relacionados con condenas y delitos. En este último caso, se nos menciona la expresión “gran escala” concepto que genera bastantes dudas, ya que el RGPD no define ni que significa, ni que alcance tiene, por ello, estamos a la espera de que la UE se pronuncie e indique la interpretación correcta del término. Mientras tanto, se ha hablado de umbrales y escalas, pero todo son meros comentarios. De momento, se está tomando como referencia la cantidad de personas afectadas, el volumen de los datos, la duración del tratamiento y el alcance geográfico.

Por último y como otro caso de obligatoriedad de nombramiento de un DPO, el Reglamento exige la designación de esta figura a las empresas que tengan más de 250 trabajadores. No obstante, aquellas que tienen menos trabajadores, lo requerirán sólo cuando para el ejercicio de su actividad les sea necesario realizar un seguimiento sistemático y periódico de datos personales.

ISSN: 1794-9920 Julio – Diciembre de 2018
Volumen 18 Número 2, Año 2018 Págs. 78 - 96

A continuación, el RGPD nos dice que si después de todo lo expuesto, definitivamente no es necesario designar un DPO, en todo caso, la labor de la protección de los datos se le debe encargar a alguien, es decir, tanto la adaptación como la supervisión debe depender de alguna persona, con lo cual, se hace necesario designar a alguien que se encargue del tema. En todo caso, el Reglamento otorga a los Estados miembro la posibilidad de exigir el nombramiento obligatorio de un DPO en circunstancias distintas a las estipuladas en el mismo dentro de sus respectivas reglamentaciones internas.

Dicho esto, hemos de advertir que el DPO debe tener conocimientos especializados en protección de datos, si bien es cierto que de momento no se esta pidiendo ningún tipo de certificación o acreditación específica, también es cierto que no se puede nombrar un DPO neófito en la materia. Además de tener estos conocimientos es necesario que conozca la empresa u organización para la que va a trabajar, prestando especial atención en los posibles riesgos propios de la actividad empresarial. Por lo general se esta recomendando que la persona destinada a ser DPO tenga conocimientos jurídicos, en cuanto que, si partimos de la base que nos exige la debida protección de los datos, nos referiremos a un reglamento, que no deja de ser un documento de carácter legislativo a nivel europeo, esto es, en palabras sencillas una Ley de obligatorio cumplimiento. No obstante, el conocimiento jurídico debe venir acompañado de un conocimiento técnico de las nuevas tecnologías y sistemas digitales, en cuanto que, la gran mayoría del tratamiento de los datos se hace mediante sistemas automatizados, es decir, utilizando mecanismos informáticos.

En cualquiera de los casos el DPO debe tener la capacidad de gestionar los registros de actividades, establecer las medidas técnicas y de seguridad, estudiar el análisis de riesgos realizado, establecer los procedimientos a realizar a la hora de tener una brecha de seguridad, realizar las evaluaciones de impacto pertinentes, mantener relación con las autoridades que supervisan su trabajo y con aquellas otras que supervisan la protección de datos misma de la empresa para que trabaja o colabora y, por último formar y sensibilizar a todo el persona en materia de protección de datos[15], cuestiones que al fin y al cabo son sus funciones, las cuales se encuetnran reguladas en los artículos 35, 37 y 38 RGPD.

Por último, he de mencionar el encaje del DPO dentro de la empresa, ya que éste puede ser parte de la misma, es decir, uno de los trabajadores o puede ser externo. En el caso en que sea un trabajador interno, éste puede seguir desarrollando sus funciones habituales y ser DPO, caso en el cual nos encontrariamos bajo una relación laboral empresa-trabajador o; un externo que preste sus servicios, caso en el cual, prestará los servicios bajo la figura de arrendamiento de servicios. En este último caso, el DPO debe tener la capacidad de desempeñar sus funciones de manera independiente. En cualquiera de las modalidades elegidas, el DPO siempre y en todo caso rendirá cuentas ante altos cargos directivos o la cúpula de la empresa.

Además, los DPO independientemente de que sean internos o externos, de acuerdo al artículo 38 RGPD gozan de indemnidad, no puededn ser destituidos ni sancionados por el sólo hecho de desempeñar sus funciones, excepto se trate de negligencia grave o dolo. Todo ello, siempre y cuando, estén cumpliendo funciones de DPO, ahora bien, si se trata de funciones distintas dentro de su contrato laboral o de arrendamiento de servicios e incurre en faltas que de acuerdo a la potestad sancionadora del empresario y la normativa vigente se castigan con destitución, cesará aquel beneficio.

### 2.1.2 Crear un Registro de actividades de tratamiento

En cuanto al registro de actividades de tratamiento, lo primero que hemos decir es que, no es obligatorio para las empresas que tengan menos de 250 trabajadores, excepto en los casos en que, el tratamiento pueda generar un riesgo, que no sea ocasional, para los derechos y libertades de los interesados; o el tratamiento incluya datos especialmente protegidos o datos referentes a condenas e infracciones penales.

Dicho esto, lo que está ocurriendo en la práctica es que todos están realizando un registro de actividades de tratamiento, ¿Por qué? Porque es la manera de identificar qué datos se tienen y para qué se están utilizando, es una manera de encuadrar dentro de diferentes clasificaciones estipuladas por la empresa, que como veremos se realizan *ad hoc* para cada una.

Entonces, cuando nos proponemos a realizar un registro de actividades de tratamiento, lo primero que debemos tener en cuenta son los nombres y datos de contacto del responsable o el representante del responsable y del DPO. A renglón seguido, la finalidad para la que se están tratando los datos personales, materialmente esto se hace de la siguiente manera, primero el encargado de la protección de datos debe realizar un diagnóstico consistente en observar y anotar o apuntar, qué datos se están tratando y cómo se están tratando los mismos, qué tipo de registro se esta llevando, si es que lo hay, cómo se está organizando, que estructura se tiene y, cómo se utilizan estos datos, todo ello con la única finalidad de organizarlos de tal manera que su gestión sea sencilla y ágil. También es importante tener en cuenta los datos que posiblemente se puedan transferir a un país u organización

[15] Varias de estas cuestiones hacen parte de otras de las medidas internas que analizaremos en los epígrafes posteriores.

internacional; los plazos estipulados por la empresa para suprimir determinados datos; las medidas técnicas y de seguridad previstas. Ahora bien, en caso de contar con un caos de datos se deben tomar las medidas necesarias para identificarlos, localizarlos y organizarlos, ya que si no se realiza este paso no podemos continuar al siguiente.

Para solventar la organización de nuestros datos podemos empezar por realizar una clasificación, por ejemplo, de acuerdo a los sujetos, es decir, de acuerdo a los usuarios o las personas de quienes tratemos sus datos o, de acuerdo a el objeto, es decir, de acuerdo al objeto de utilización de sus datos, el para qué utilizamos sus datos. Posteriormente, verificaremos la información y es importante hacer hincapié en las siguientes cuestiones: primera identificar si estos datos están correctamente recogidos, si se han recogido con el consentimiento y las exigencias debidas y; segunda, si la clasificación donde se encontraban es la correcta de acuerdo a nuestro orden o es necesario cambiarlos de sitio.

En todo caso en el registro de actividades de tratamiento y siguiendo la organización proporcionada por la Agencia Española de Protección de Datos debe contener: 1. El nombre y los datos de contacto del responsable, corresponsable o representante del responsable, 2. Nombre y datos de contacto del DPO, 3. La finalidad expresa con la respectiva fundamentación jurídica que explique el para qué se están utilizando estos datos, 4. Las categorías de personas tanto físicas como jurídicas, en fin, todas aquellas de las que se traten datos, perfectamente identificadas o identificables, por ejemplo, clientes, empleados, proveedores, gestores, etcétera, 5. Las categorías de los datos, en este aspecto se recogen los detalles de todos los datos, bien si son identificativos, bien si son financieros, profesionales o cualquier otro, como punto 6, mencionaremos las transferencias y cesiones, la cesión de los datos como mencionamos anteriormente a otro país o a una organización internacional; la transferencia de datos, el período de conservación de los mismos y, las medidas técnicas y de seguridad.

### 2.1.3 Realizar un análisis de riesgos

El tercer paso es realizar un análisis de riesgos, para el cual sé toma como referencia el Registro de Actividades que ya se ha constituido. Pues bien, dentro del mismo los que se trata es de gestionar los riesgos, mediante un proceso que permita identificar cuáles son los posibles riesgos y amenazas a las que están expuestos nuestros datos y; analizar y valorar qué consecuencia tendrían las mismas si se llegan a materializar.

Pues bien, los riesgos los podemos clasificar en riesgos para los usuarios afectados, es decir, el conocimiento de datos e información de los datos que se están tratando; riesgos de carácter empresarial, cómo, por ejemplo, la pérdida de reputación y/o las sanciones derivadas de una quiebra de seguridad y, los riesgos derivados del propio incumplimiento de la normativa referente a protección de datos.

De otro lado, amenazas pueden ser de cualquier tipo, por ejemplo, amenazas informáticas o físicas y en cualquier tipo de modalidad, no debemos subestimar la mente de quien se encarga de proteger los datos, ya que por disparatada o sencilla que nos parezca la amenaza, con el sólo hecho de que exista una posibilidad de su consecución, nuestros datos peligran, lo que ocurre es que como voy a explicar a continuación, existe una clasificación, sin embargo, ésta la podemos aumentar con nuestros propios *items,* en consonancia con nuestra labor o, incluir varias de nuestras amenaza dentro de las clasificaciones.

Entonces, ¿Cuáles son los factores de riesgo que pueden llegar a provocar daños o perjuicios a los interesados? Básicamente, estas amenazas pueden ser de tres tipos: la primera el acceso ilegítimo a los datos, que provocaría que los datos fueran conocidos por quien no debe conocerlos; la segunda, la modificación no autorizada de los datos y aquí es donde cabe preguntarse ¿qué pasaría si un dato es modificado sin la autorización debida? Y; tercera, la eliminación de los datos, esto es ¿qué ocurriría en el caso en que no se tuviera o no se pudiera utilizar un dato? No obstante, no basta con analizar cuáles son los factores de riesgo, también hemos de analizar cuál es el impacto de la generación o realización de estos factores, ya que este último análisis es el que verdaderamente nos va a llevar a establecer el grado de riesgo de nuestras posibles amenazas. Por un momento, nos tenemos que deterner a pensar cuál es la gravedad del efecto generado por la producción de la amenaza, ya que este proceso es el que nos permite catalogar las amenazas y clasificarlas de acuerdo a su impacto. Además, la meritada clasificación nos va a marcar la hoja de ruta a la hora de tomar las medidas necesarias para que el impacto de nuestras brechas de seguridad sea el menor posible. Aunque tenemos que admitir que el riesgo cero no existe, siempre tendremos riesgos, ahora bien, este ejercicio lo que permite es que el meritado riesgo se pueda disminuir a terminos razonables, pero nunca lo elimina.

### 2.1.4 Realizar una evaluación de impacto

El cuarto paso es realizar una evaluación de impacto del riesgo, que no es otra cosa que un paso con carácter preventivo, que debe realizar quien esté como responsable

del tratamiento de datos, con la finalidad de identificar, evaluar y gestionar los riesgos a los que está expuesto nuestro Registro de Actividades. Este paso, lo que permite es una vez identificado el riesgo y las posibles amenazas y, segmentados los datos personales, se determine el nivel de riesgo, a través, de una escala creada por quién esté encargado de los datos. Todo ello con el objetivo de que sea más fácil elegir las medidas a tomar, para proteger los datos y evitar un quebrantamiento o brecha de seguridad, intentado reducir los riesgos al menor nivel posible.

Esta evaluación no tiene un criterio definido en lo que respecta a la mayor o menor posibilidad de riegos, se deja al arbitrio de cada entidad, por ejemplo, se utilizan escalas de 1 a 10, variaciones en mayor, medio o menor riesgo. Tampoco se define exactamente, qué datos tienen más riesgo que otros, porque dependerá de la finalidad para la que se tratan. Como ejemplo podemos tomar una clínica privada que cuenta con los servicios de trabajadores provenientes de una agencia de colocación y, por tanto, maneja sus datos. En este caso, puede que tengan mayor relevancia y peligro o riesgo los datos de estos trabajadores en la agencia de colocación que en la clínica privada, por cuanto, la actividad principal de la clínica privada es atender pacientes, mientras que la actividad principal de la agencia de colocación, es buscar ofertas de empleo y buscar trabajadores que cumplan con los requisitos de las mismas y realizar el contacto entre unas y otras. En fin, las evaluaciones tienen un criterio distinto de acuerdo a donde se aplican.

Dicho esto, analizaremos ¿cuál es el contenido de la evaluación de riesgos? La evaluación, además de la escala creada y determinada ad hoc para cada empresa debe contener, la descripción metódica y periódica del tratamiento, ya que en muchos casos el interés legítimo que tenía el responsable por determinados datos puede desaparecer; la evaluación de los riesgos que puedan tener los datos, esto con la finalidad de proteger los derechos y libertades de quienes se tienen los datos, también se debe evaluar la necesidad de esta evaluación de riesgos, en este aspecto se debe analizar si el tratamiento es proporcional respecto de la finalidad para la que se están tratando datos y, por último se deben incluir las medidas con las que se cuentan para afrontar las situaciones de riesgo.

Una vez explicado el concepto y el contenido de la evaluación de riesgos, hemos de advertir que la misma, no es necesaria en todos los casos. De conformidad con el artículo 35 RGPD, es necesario realizar la evaluación de impacto en los casos de: 1. “evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar […]; 2. “tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o […]” y, “observación sistemática a gran escala de una zona de acceso público.”

Además de estos casos, el RGPD establece que aparte de los tres casos que trae regulados el mismo, también las autoridades de control podrán regular casos, elaborando y publicando unas listas de operaciones que requieran de la realización de una evaluación de impacto, con lo cual, habrá que estar pendientes de cada una de las regulaciones nacionales, para saber si nuestra actividad se encuadra en uno de los casos regulados. Cabe resaltar que las mencionadas listas deben contener los casos definidos y detallados, así como que deben estar documentadas y ser validadas por el Comité Europeo de Protección de Datos.

Posteriormente, si definitivamente quien trata los datos no encuadra dentro de ninguno de los casos que explicamos, en todo caso, cabe hacer un análisis de necesidad de la evaluación de impacto, sea que terminemos haciendo la evaluación o no, siempre tendremos que justificar y documentar porque se hace o no se hace, con lo cual, no está demás. Para ello, en primer lugar debemos analizar la naturaleza de los datos que tratamos, esto es, analizar si nos encontramos frente a categorías de datos especialmente protegidos, si manejamos datos a gran escala o si los datos pertenecen a personas en situación de vulnerabilidad. Además de ello, debemos analizar el alcance del tratamiento de los datos, ya que debemos pensar en los efectos y las consecuencias que puede traer una brecha de seguridad, situación que nos llevará a identificar el nivel de riesgo frente al que nos encontramos; unido al tema del alcance, también es importante tener en cuenta el contexto, ya que no debemos analizar las situaciones aisladamente sino el conjunto de circunstancias bajo las que se realiza el tratamiento, también para verificar el nivel de riesgo y, finalmente, analizar de acuerdo a las finalidades para las que se están tratando los datos, el nivel de riesgo en el que nos podamos encontrar.

Finalmente, si es necesario realizar la evaluación se ha de realizar de acuerdo a lo establecido al menos en el caso español, en la “Guía de Evaluación de Impacto en la Protección de Datos” de la Agencia Española de Protección de Datos, asumimos que en los demás países de la UE existen organismos homólogos a ésta que se han encargado de crear estas guías. Ahora, si no es necesario llevar a cabo la evaluación de impacto entenderemos que nuestra actividad no está expuesta a riesgos tan relevantes, sin embargo, también es necesario justificar y documentar los motivos por los cuales se entiende que no es necesario llevar a cabo la misma.

### 2.1.5 Las medidas

El quinto paso es recabar las medidas de seguridad que se tienen, ya que la antigua Ley Orgánica de Protección de Datos las traía recogidas a medidas, esto es, para cada caso había una medida determinada. Sin embargo, el RGPD no hace lo mismo, a *sensu contrario* deja abierta la posiblidad a la toma de medidas por parte de los obligados a proteger los datos, es más, con anterioridad al Reglamento las medidas estaban basadas en el tipo de datos tratados con una que otra matización, ahora bien, con la nueva regulación exige mayores variables. Insistimos en que el Reglamento no especifica qué tipo de medidas hay que tomar, lo deja a decisión de las empresas. Poor ejemplo, en el caso español se ha experimentado un cambio en lo referente a las medidas, ya que en la LOPD las medias a tomar venían tasadas mientras que con el Reglamento como hemos dicho se toman las que a bien se tienen por cada empresa, es más, incluso en la nueva Ley 3/2018, de 5 de diciembre de protección de datos personales y garantía de los derechos digitales tampoco se promueve ningún tipo de medida.

Ahora bien, dichas medidas deben ser técnicas y organizativas y se pueden traducir de forma física o electrónica dependiendo de los formatos en los que reposan los datos. No obstante, cabe resaltar que en los casos en que se habían tomado las medidas de acuedo a las regulaciones antiguas, se podrán mantener las mismas, siempre que se pueda demostrar que las mismas son las más adecuadas y optiamas para el respectivo tratamiento de los datos. Todo ello, sin olvidar que en la gran mayoría de los casos será necesario complementar las mismas con otras adicionales para prestar el nivel de seguridad adecuado.

De otro lado, para abordar el tema de las medias expresaremos alguans que nuestro modo de enenteder han resultado beneficiosas para determinados casos, por ejemplo, centremonos en un despacho de abogados en el que habitualmente tenemos un archivo físico y otro electrónico, en estos casos es necesario establecer medidas para proteger los meritados archivos. En el caso el archivo físico conviene que este cerrado bajo llave o clave de seguridad, que se tenga un inventario del mismo, que quienes acceden a él sean personas autorizadas entre otras. A su vez, en lo referente al archivo electrónico conviene que el acceso a la información requiera de alguna clave, la información que reposa en “nubes” esté encriptada, que se cuente con una copia de seguridad y tantas otras medidas, las cuales, se entienda que cooperarán para realizar una protección efectiva de datos.

Existen otras medidas que se suelen tomar, por ejemplo, poner clave de acceso a los ordenadores y en caso de tener un servidor remoto, claves de acceso remoto; si se tiene un disco duro externo, dejarlo bajo custodia de alguna persona que lo vigile en todo momento o simplemente dejarlo bajo llave. En fin, cualquier tipo de medida que se crea va a evitar que la amenaza se materialice, se debe tomar por peculiar que parezca, insisto en la peculiaridad porque cada cual conoce su empresa y no todas son iguales, con lo cual, en unas empresas habrá que tomar ciertas medidas que no se toman en otras. En un sin número de casos, las personas se toman este tema jocosamente, sin embargo, en la mayoría de veces por simples o estrambóticas que parezcan las ideas, son éstas las que nos dan un poco más de tranquilidad e incluso puede ser claves y determinantes al momento de sufrir un ataque cuya consecuencia sea una brecha de seguridad.

En este tema puntual la casuística es la que nos va guiando sobre las nuevas formas de intentar generar brechas de seguridad, asi por ejempo, encontramos varios casos de vulneración de la página web; infecciónes por un fenómeno llamado *ransomware* que consiste en qué un determinado usuario se secuestra un sistema o determinada información y exige un pago como “rescate” para que la información retorne a su antiguo dueño. En esto casos es curioso pero ocurre en la gran mayoría de ocasiones por el propio descuido de los trabajadores, que en un sin número de casos caen en estas trampas por falta de formación y de conocimiento al respecto. Así, los secuestradores de información, a través de un programa informático cifran los archivos y restringen el acceso a los mismos, cuando ya los tienen exigen un rescate pero para evitar el rastreo de cuentas y demás, nos hemos encontrado con varios casos en los que el rescate se debe pagar en formato *bitcoin.* También es habitual encontrar IP infectadas desde las cuales se pueden producir ciberataques a distintos clientes, para ello, la solución más frecuente corresponde a establecer políticas de *firewall.* Sin embargo, es de las amenzanas más difíciles de superar, en cuanto, que normalmente los ordenadores que utilizan una misma IP son muchos e incluso están distribuidos geográficamente en varios lugares, con lo cual, combatir esta amenaza es muy complicado. Además otro de los casos puntuales de mayor riesgo es el tema de las criptomonedas o *bitcoins*.

Frente a todos estos riesgos, las medidas que se han tomado han sido la actualización constante de los sistemas operativos y los navegadores utilizados; la instalación y actualización períodica, incluso en algunos casos automática de antivirus y *firewall;* la limitación del acceso a determinadas cuentas de usuario, a las cuales, en principio accedera sólo el adinsitrador y exepcionalmente otro usuario y, en todo caso el acceso será restringido y controlado; la utilización de contraseñas más elaboradas que contengan además de letras, números, símbolos etcetéra; la actualización períodica de

ISSN: 1794-9920 Julio – Diciembre de 2018
Volumen 18 Número 2, Año 2018 Págs. 78 - 96

las mismas; la precaución al a hora de descargar programas de internet y ejecutar los mismos, incluso la precaución frente a los dispositivos de almacenamiento USB que deben ser escanéados antes de su utilización. Asimismo, en varias empresas los dispositivos electrónicos utilizados que en su gran mayoría son ordenadores, no tienen puertos de ningún tipo evitando así la fuga de información o sólo lo tienen determinados empleados a quienes se les considera necesitan para cumplir sus funciones de este tipo de puertos de acceso. En lo referente a las aplicaciones descargadas en dispositivos móviles es pertienente que las mismas correspondas an marcas reconocidas, sobre todo cuando se trata de tabletas y móviles de la propia empresa que utilizan determinados empleados.

Por último y como caso puntual cabe destacar en los casos de marcas e imagen propia posicionada en redes sociales o portales web, la supervisión de las mismas en todas las redes, así como, de su contenido y funcionamiento para evitar posibles supuestos de suplantación, publicación de información, ofertas, servicios falsos, erroneos o dispares que generen confusión y desconfianza a nuestros clientes.

#### 2.1.6. Mecanismos y procedimiento de notificación a los usuarios

Como sexto y último paso se deben establecer los mecanismos y el procedimiento de notificación a los usuarios que se va a utilizar en el momento en que exista una brecha o quiebra de seguridad, entendida ésta como cualquier incidente que ocasione la perdida, alteración ilícita o destrucción de datos personales, situaciones que se pueden materializar, por ejemplo, con el acceso no autorizado a una base de datos o la perdida o robo de un ordenador, e incluso la supresión accidental de datos. Cuando ocurren estas situaciones, lo primero que debe hacer el responsable de protección de datos es notificar a la autoridad de protección de datos competente, en el caso español, la Agencia Española de Protección de Datos, excepto se entienda que dicha brecha no genera una violación de los derechos y libertades de las personas dueñas de los datos que han sufrido el percance. Ahora bien, en los casos en que se genere una violación se deberá notificar también las personas que han sufrido las consecuencias de la brecha, esta última notificación lo que permite es que las personas afectadas puedan ejercitar sus derechos frente al responsable de la protección de sus datos.

El procedimiento de notificación, así como varias de las cuestiones a las que se refiere el RGPD son de libre elección, por tanto, se puede utilizar desde un mensaje de texto hasta un correo electrónico. El hecho es que las personas de quienes se tienen los datos sepan que ha habido una quiebra de seguridad. Lo único que nos exige el Reglamento es que la notificación de dicha brecha sea realizada en el plazo máximo de 72 horas después de que el responsable se ha percatado de la misma. En dicha notificación es importante que se incluya, la naturaleza de la violación, las categorías de datos, las medidas adoptadas frente a la quiebra de seguridad y, si se ha podido aplicar alguna medida de las estipuladas, especificar cómo y cuándo se ha aplicado. En caso de que no sea posible realizar la notificación dentro del plazo estipulado, la misma se realizará en la mayor brevedad posible y adjuntando una nota explicativa de los motivos por los cuales no pudo ser notificada dentro del plazo. Además, en los casos en que la notificación pueda suponer un esfuerzo desproporcionado se puede acudir a la comunicación pública.

En todo caso, todas las brechas de seguridad deben ser documentadas, desde que ocurren hasta que terminan, incluyendo las respectivas notificaciones a la autoridad de protección de datos competente, así como a los interesados, si fuere necesario y, las medidas aplicadas.

### 2.2 Pasos externos

Dentro de este apartado estudiaremos cada unos de los pasos externos que deben realizar todos quienes tratan datos, para adaptarse al RGPD. Los definimos como pasos externos porque se constituyen como la secuencia de actos que deben realizar las empresas; los autónomos, en fin, cualquiera de los obligados a adecuarse al RGPD por el tratamiento que lleva de los mismos. Los llamamos externos ya que son conocidos por personas en principio externas al tratante de datos, especialmente los usuarios, en lo que respecta a el ejercicio de sus derechos y a la política de privacidad. De otro lado, en lo referente a las condiciones de los contratos de posibles colaboradores que veremos más adelante, hemos de resltar que lo incluimos en pasos externos porque en muchos casos estas personas pueden ser externas a la empresa más no por los usuarios o consumidores de los servicios ofertados.

#### 2.2.1 Captación del consentimiento y Derechos de los usuarios

El primero de los pasos externos es recabar el consentimiento de las personas que nos ceden sus datos personales, el Reglamento nos dice que debeos recabar el consentimiento, pero no nos dice cómo lo debemos hacer, por tanto, nos encontramos frente a una nueva situación de libre elección. Las empresas, por ejemplo, se preguntan ¿se puede recabar el consentimiento de forma oral? En principio el Reglamento como mencionaba anteriormente

es marco, sobre la oralidad no dice nada, sin embargo, lo que exige es que se pueda demostrar que el consentimiento se ha recabado. Pues bien, dentro de este primer paso lo que se debe hacer es adaptar o adecuar los formularios en los que estamos recabando el consentimiento de los usuarios. Habitualmente, estos se documentan, ahora bien, si existe algún otro mecanismo para demostrarlo el Reglamento no se opone, al contrario, lo acepta. El hecho es poder demostrarlo.

Además de recabar el consentimiento, se debe informar a los usuarios sobre sus derechos, aquí aparecen los llamados derechos ARCO, esto es, el derecho de acceso, rectificación, cancelación y oposición. Hemos de decir que dentro de este Reglamento se está regulando el Derecho al olvido que lleva siendo tema de discusión y reclamo de una parte del sector de la sociedad desde hace años y como novedad nos trae el Derecho a la portabilidad.

El Derecho de acceso consiste en que los usuarios tienen derecho a conocer si sus datos están siendo utilizados y para qué están siendo utilizados. En caso de ser afirmativa la respuesta, también se les debe informar cómo han sido recogidos, con qué finalidad, cuando y para qué han sido utilizados, es más, tienen derecho a que se les entregue una copia de los mismos. En lo referente a este Derecho, el Reglamento establece un plazo de 30 días para que quién tenga los datos contestes al usuario sobre su solicitud, y a su vez después de contestado concede un plazo de 10 días hábiles para que el usuario los pueda consultar. Otro de los derechos es el Derecho de rectificación consistente en que los usuarios pueden solicitar la modificación del os datos, bien porque sean incorrectos, bien por que sean inexactos mediante una solicitud y aportando documentación que justifique la modificación. Asimismo, los usuarios cuentan con el Derecho de oposición que consiste en oponerse al tratamiento de sus datos justificándolo mediante motivos fundados y legítimos. Finalmente, el Derecho de cancelación, mediante el cual, el usuario puede solicitar que se supriman sus datos personales cuando resulten inadecuados o excesivos para los fines que se han recogido. En la solicitud se debe indicar el dato y el motivo por el cual debe ser suprimido siempre aportando documentación justificativa. El plazo para contestar las solicitudes de los tres últimos Derechos es de 10 días hábiles.

Además de estos Derechos, el reglamento ha incluido el Derecho al olvido y el Derecho de Portabilidad, el derecho al olvido como mencionaba es la gran novedad, el mismo consiste en que los datos de los usuarios se supriman en los siguientes casos: 1. Cuando ya no sean necesarios conforme a su finalidad; 2. El usuario retire el consentimiento; 3. El usuario ejerza el derecho de oposición sobre los datos o éstos sean tratados de forma ilícita; 4. Los datos no sean necesarios en relación con los fines para los que fueron recogidos o fueron tratados de otro modo; 5. El interesado retire el consentimiento en que se basa el tratamiento y éste no se base en otro fundamento jurídico; 6. el interesado se oponga al tratamiento con arreglo al Derecho de oposición, por motivos particulares o por mercadotecnia y no prevalezcan otros motivos legítimos para el tratamiento, por ejemplo, el tratamiento ilícito de datos; 7. La supresión de los datos en cumplimiento de una obligación legal o se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

Finalmente, el Derecho de portabilidad facilita al usuario la posibilidad de solicitar sus datos personales en un formato estructurado en el caso en que desee cambiar de prestador de servicios.

Asimismo, se debe informar sobre los procedimientos establecidos por cada entidad o empresa para el ejercicio de los mencionados Derechos, ya que, en lo referente a este tema, el Reglamento tampoco establece un procedimiento determinado. Por esta razón, algunas empresas solicitan la fotocopia del documento de identidad, la solicitud de ejercicio del Derecho, la documentación justificativa y una dirección para notificaciones.

### 2.2.2 Contratos de los encargados del tratamiento de datos

El segundo paso interno a tener en cuenta es los contratos que se celebran con el o los encargados del tratamiento de datos, por ejemplo, delegados de protección de datos, responsables, encargados etcétera. En estos contratos es importante específicar y establecer con claridad y detalle las funciones de los mismos; el tipo de tratamiento de datos del que se va a hacer cargo; las instrucciones que va a recibir y aquellas que debe dar; el nivel de decisión que puede asumir el encargado; el deber de confidencialidad; las medidas de seguridad que debe aplicar, los procedimientos referentes a los derechos de los interesados, los informes o las formas de demostrar el cumplimiento de sus funciones y obligaciones, en fin, todos los detalles y por menores del contrato que en lo posible deben ser lo mas exhaustivos posibles.

En este punto es importante hacer un comentario, en muchos casos estas personas son elegidas de entre los trabajadores de la misma empresa y en otros tantos, se contratan personas externas para estas funciones. Pues bien, de uno u otro lado, es con absolutamente necesario celebrar un contrato específico, en el que se observen con especial detenimiento las cláusulas sobre los temas mencionados, así como que, quien se dedicará a estas cuestiones quede perfectamente enterado de sus

obligaciones y las responsabilidades que atañen al cargo. Todo esto, porque estamos hablando de una cuestión bastante delicada, los Derechos de intimidad y honor, entre otros de las personas, traducidos y garantizados a través de la protección de datos. Además de la responsabilidad, existen profesiones donde es obligatorio guardar el secreto profesional, ya que hace parte de la práctica de las mismas, pues bien, en estos casos con mayor exhaustividad aún se deben observar las meritadas cláusulas. Recordemos que, en un sin fin de casos, las brechas de seguridad las han provocado antiguos trabajadores de los lugares donde reposan los datos, pues cuanto más, aquellos que los tratan directamente y tienen acceso a ellos aunque sea durante un tiempo. Tenemos que tener la certeza de que sí una de las personas que ocupa estos cargos, bien nos abandona o bien la despedimos, no va a poder de ninguna manera generar una brecha de seguridad o al menos le va a costar demasiado, de lo contrario seremos víctimas de la materialización de amenzas por parte de nuestro antiguo personal o antiguos colaboradores.

**2.2.3 Adaptación de la política de privacidad**

El tercer y último paso que se debe realizar es adaptar la política de privacidad de las empresas, a través de los mensajes al final de los correos electrónicos, la página web, entre otros. En este punto consideramos importante referirnos a tres aspectos, el primero las páginas web junto con el uso de cookies dentro de las mismas y las comunicaciones comerciales de carácter electrónico.

En lo referente a las páginas web podemos iniciar diciendo que quién a día de hoy no tiene una página web prácticamente no existe para el mundo, con lo cual, casi todas las empresas tienen una. Pues bien, a través de la misma se ofrecen servicios, se envían comunicaciones etcétera. En todos estos casos, además de cumplir el RGPD en el caso español se deben cumplir también los requisitos establecidos en la Ley 34/2002, de Servicios de la Sociedad de la Información entratandose de comunicaciones comerciales.

A su vez, de acuerdo al artículo 10 del mismo precepto en la página web está " [...] obligado a disponer de los medios que permitan, tanto a los etinatarios del servicio como al os órganos competentes, acceder por medios eletrónicos, de forma permanente, fácil, directa y gratuita [...]" a la información correspondiente a nombre o denominación social, el domicilio, un correo electrónico y, cualquier otro dato que permia una comunicación directa y efectiva con el establecimiento; los datos de inscripción en el Registro Mercantil o en el registro en el qué por motivo de su actividad se encuentren inscritos; para los casos en que la actividad esté sujeta a un régimen de autorización administrativa previa, se deben incluir los datos relativos a la autorización y la identificación del órgano competente de su supervisión; en los casos en que se ejerza una profesión regulada se deben indicar los datos del Colegio Profesional al que pertenece y su número de colegiado; el título académico oficial o profesional que le habilita como tal; el Estado de la UE o del Espacio Económico Europeo que expidió el título profesional y en los casos que corresponda, la homologación o reconocimiento y; las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se pueden consultar; el número fiscal y; en los casos en que se haga referencia a precios, se debe facilitar una información clara y exacta sobre el precio del producto o servicio, indicando en todo caso, si incluye o no los impuestos aplicables y/o los gastos de envió. Por último, también se deben incluir los códigos de conducta a los que esté adherido si es que es el caso y la forma de consultarlos eletrónicamente.

Además en los casos en los que se tenga una línea de atención teléfonica que tenga algún coste, la utilización de la misma, así omo, la descargade programas informáticos que efectuén funciones marcanción, deben realizarse con el previo consentimiento, inforado y expreso de quien pretende usuarlos.

De otro lado, también se deben estipular los procedimientos de recogida de datos en la web, bien en formularios de contacto o consulta, en los cuáles, debe quedar plenamente recabado el consentimiento de acuerdo a la normativa vigente. Además se deben publicar todos los datos y formularios, así como, procedimientos existentes para que los usuarios puedan ejercitar sus Derechos.

En segundo lugar y en lo que respecta a las comunicaciones comerciales de carácter electrónico, en términos generales y acudiendo a la legislación española como base, se prohíbe el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación, entiendase, SMS, mensajería instantanéa, etc; en los casos en que no haya sido expresamente autorizado por los destinatarios, excepto en los casos en que exista una relación contractual previa y mientras el prestador de servicios hubiere recabado los datos lícitamente. En todo caso, es necesario que los usuarios encuentren dentro de las comunicaciones una opción que les permita darse de baja o no volver a recibirlas, si es que así lo desean. Debe aparecer algún tipo de opción o un correo electrónico que les permita ejercitar su derecho a no recibir más comunicaciones por parte de determinado prestador de servicios.

En lo que respecta a los identificadores de sesión o más conocidos como "cookies", la legislación permite que en las páginas web se utilicen dispositivos de almacenamiento y recuperadores de información de este estilo en los equipos utilizados por los destinatarios, en la medida en que, se les informe de manera clara y completa la utilización de los dispositivos de almacenamiento y los fines del tratamiento

de acuerdo a lo dispuesto en el RGPD y éste haya prestado su consentimiento. Para que la política de "cookies" se adapte al RGPD debe ser transparente, debe haberse obtenido el consentimiento previo mediante una acción afirmativa evidente, por ejemplo, el usual "acepto el uso de cookies", así como, se debe permitir el rechazo del uso de dicha política y; se debe estipular la opción o posibilidad de retirar el consentimiento en cualquier momento.

## 4. Hacía donde vamos ¿Cuál es el futuro?

Europa se encuentra tratándose de adaptar, de un lado los usuarios recibiendo comunicaciones constantes de actualización de la política de privacidad de datos, además, se está enterando de los Derechos que tienen frente a las empresas. Los usuarios están haciendo preguntas y adaptándose a la aplicación de esta nueva regulación que en el fondo atañe a todos y cada uno de los ciudadanos. De otro lado, las empresas en su gran mayoría ya han iniciado todas las labores para adecuarse, unas más que otras, pero al final todas lo tendrán que hacer, todo ello, lo único que nos puede llevar a pensar es que aún se encuentra en fase adaptación y por tanto de transformación.

Ahora bien, ¿Cuál es el futuro? ¿hacía dónde va Europa? Los países europeos están modificando o derogando sus actuales Leyes de Protección de Datos con la finalidad de crear otras nuevas que se adapten al Reglamento. En España, por ejemplo, si bien es cierto que la nueva Ley Orgánica de Protección de Datos tardó en salir 6 meses después de que se hiciera obligatorio el RGPD, ya que tuvimos cambio de gobierno a mediados de 2018 y, entre otras cuestiones se presentaron casi 400 enmiendas al Proyecto de Ley. Entre medias y para mitigar la urgencia de la Ley, el Parlamento español aprobó el pasado 6 de septiembre el Real Decreto-Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la UE en materia de protección de datos, reforzando varios temas, por ejemplo, el consentimiento prestado por los usuarios deberá ser activo y expresamente un sí, de lo contrario no tendrá validez; además reconoció el Derecho al olvido en los casos en que los datos no sean necesarios; el usuario haya decidido retirar el consentimiento, se haya opuesto al uso de los mismos o los mismos se hayan utilizado de forma ilícita.

Además, promoviendo la figura del Delegado de Protección de Datos indicó que todos los organismos públicos deben contar con un DPO y las privadas en aquellos casos en los que el Reglamento así lo exige. A su vez, también instauró un sistema de multas en caso de incumplimiento del Reglamento, estas sanciones serán hasta de 10.000.000 de euros o hasta el 2% del volumen de negocio, si se trata de una empresa.

Aparte del Real Decreto-Ley y mientras la nueva Ley era aprobada tuvimos un debate nacional consistente en la posible inclusión de los llamados Derechos digitales, esto es, el acceso universal a internet, el Derecho a la desconexión o el testamento digital, entre otros, en la Ley Orgánica de Protección de Datos o su definitiva regulación una Ley distinta y paralela a ésta. Pues bien, en nuestro concepto, nos decantabamos por pensar que la protección de datos es una cuestión distinta a los Derechos digitales, no obstante, la misma tiene su fundamento en la Constitución Española de 1978 que en su artículo 18 recoge el derecho a la intimidad, es por ello, que entendemos que la protección de datos es más que un Derecho digital, cuando hablamos de protección de datos estamos mencionando una cuestión que atañe a Derechos fundamentales recogidos en la carta magna, mientras que cuanto hablamos de Derechos digitales no necesarimanete nos referimos a este tipo de Derechos. Además, considerabamos que nos encontramos frente a dos procesos distintos, de un lado la adaptación de la legislación española a la legislación europea y otro un proceso distinto es la adaptación de los Derechos y libertades constitucionales al mundo digital que debe hacer el Estado español.

Finalmente, en el mes de diciembre del 2018 fue aprobada la nueva Ley española de Protección de Datos, en la cual aparte de recoger la regulación sobre protección de datos, también se recogen los Derechos digitales. Además, trae cambios frente a la antigua regulación y novedades propias del marco de actuación que deja el propio Reglamento. Entendemos oportuno e importante destacar algunos temas, tales como, la regulación del testamento digital, para los casos en que los familiares o herederos de personas fallecidas pretendan acceder, solicitar la supresión o rectificación de los datos del mismo; el sistema de denuncias internas que ahora serán anónimas, se específica la figura del DPO, en cuanto a los requisitos para optar por este cargo, el mismo debe tener conocimiento jurídicos acreditados y además haber realizado algún curso de especialización; cambia el régimen jurídico de la Agencia Española de Protección de Datos; se suprimen las sanciones por incumplimiento del RGPD para el sector público y finalmente como indicamos anteriormente se incluyen los Derechos digitales. Así como ocurre en España, los demás paisés pertenecientes a la Unión Europea están en proceso de actualización y "modernización" de sus respectivas regulaciones referentes a la protección de datos.

En el caso de Alemania, llamativo porque fue el primer país en adaptarse a la normativa europea, la Ley de Protección

ISSN: 1794-9920 Julio – Diciembre de 2018
Volumen 18 Número 2, Año 2018 Págs. 78 - 96

de Datos (en alemán "Bundesdatenschutzgesetz")[16] fue aprobada en julio de 2017, esto es, casi con un año de antelación a la obligatoriedad del cumplimiento del RGPD; es distinto el caso de Francia cuya Asamblea Nacional acaba de aprobar, el pasado mes de febrero, el Proyecto de Ley de Protección de Datos que pretende adaptar la Ley sobre Tecnología de la Información y Libertades Civiles francesa de 1978[17] a la nueva regulación europea; Austria por su parte modificó la antigua Ley de Protección de Datos integrando a partir de abril de 2018 el Austrian Data Protection Act (Datenschutzgeset)[18]; por su parte Belgica aprobó su nueva Ley de Protección de Datos en julio de 2018[19]; Bulgaria modificó su antigua Ley en julio de 2018 aprobando el Personal Data Protection Act (Draft Bill)[20]; en Chipre fue publicada la Ley 125(I)/2018[21]; en el caso de Croacia la "Zakon o provedbi Opće uredbe o zaštiti podataka"[22] fue promulgada por el Parlamento Croata el 27 de abril de 2018 y entró en vigor el 25 de mayo del mismo año; Dinamarca aprobó a través de su Parlamento la Ley 502 "Danish Data Protection Act"[23] de 23 de mayo de 2018 cuya entrada en vigor fue el 25 de mayo de 2018 reemplazando así la Ley de Datos Personales del 2000; Eslovaquia aprobó su nueva Ley 18/2018 Coll. de Protección de Datos (""Slovak Data Protection Act"), el 30 de enero de 2018 y entró en vigor el 25 de mayo de 2018 sustituyendo ésta a la Ley Eslovaca Nº 122/2013 Coll de Protección de Datos Personales[24]; en el caso de Estonia la nueva Ley de Protección de Datos Personales fue aprobada el 12 de diciembre de 2018[25] y la misma entró en vigor el 15 de enero de 2019, sin embargo, cabe resaltar que debido al RGPD tuvo que ser modificado el Código Penal de este país con la finalidad de poder imponer las cantidades de las multas impuestas en el RGPD a su legislación. A la fecha se encuentra en debate legislativo el proyecyo de Ley de implementación y las enmiendas al Código Penal. En el caso de Finlandia se aprobó el 5 de diciembre de 2018 la Ley de Protección de Datos ("Tietosuojalaki")[26] y entró en virgor el 1 de enero de 2019; en el caso de Hungría se tomaron varias medidas y se modificaron varias leyes, no obstante, la Ley que adoptó el RGPD entró en vigor el 26 de julio de 2018[27], sin embargo, aún se esperan modificaciones en leyes sectoriales con la finalidad de armonizar la actual legislación húngara referente a la protección de datos con la legislación europea. Irlanda lo hizo a través de la Ley número 7 de 2018, Data Protection Act 2018[28]; Italia armonizó su marco normativo de protección de datos con el Decreto Legislativo 101/2018[29] que entró en vigor el 19 de septiembre de 2018; Letonia aprobó su Ley de Protección de Datos que entró en vigot el 5 de julio de 2018 reemplazando la antigua Ley[30]; Lituania también reemplazo su antigua Ley aprobando la nueva "Data Protection Law" que entrón en vigor el 16 de julio de 2018[31]; en el caso de Luxemburgo se aprobaron dos Leyes el 1 de agosto de 2018[32] para introducir al RGPD y además se realizaron varias enmiendas a las vigentes Leyes para en determinados casos incoroporar y otros tantos simplemente adaptar la normativa europea a la legislación nacional; Malta por su parte reemplazó su antigua Ley con la "Data Protection Act" que entró en vigor el 28 de mayo de 2018[33]; en el caso de los Países Bajos tenían una Ley de Protección de Datos que se adaptaba bastante bien el RGPD, por esta razón, decidieron para armonizar y mejorar la legislación ya existente promulgar la Ley Holandesa de implementación del RGPD (Uitvoeringswet AVG)[34] que les permite implementar las disposiciones del Reglamento cuando sea necesario, por ejemplo, en materia de autoridad en materia de protección de datos; actualmente tanto la Ley anterior como la de implementación siguen vigentes en los Países Bajos y estamos a espera de que se defina su situación para 2019; en el caso de Polonia fueron publicados dos Proyectos de Ley en septiembre de 2017, uno sobre la Ley Protección de Datos Personales y otro sobre la implementación de la Protección de Datos cuya finalidad es modificar todo el elenco de leyes de carácter sectorial, la primera Ley fue

[16] https://dsgvo-gesetz.de/bdsg/ Visitada 20/02/2019 a las 18:00
[17] https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee Visitada 20/02/2019 a las 18:00
[18] https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html Visitada 20/02/2018 a las 18:30
[19] https://iapp.org/media/pdf/resource_center/Belgian-GDPR-law_FR-DUTCH.pdf Visitada 20/02/2019 a las 18:30
[20] https://www.parliament.bg/bg/laws/ID/78179 Visitada 20/02/2098 18:31
[21] http://www.cygazette.com/Gazette.dll/%7BA732F24B-2FD0-4D3D-884D-258C507E2509%7D/AppPgView?IssueNo=4670&PageNo=0&AppNo=1&PartNo=1&IssueDate=2/1/2013 Visitada 20/02/2019 a las 18:31
[22] https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html Visitada 20/02/2019 a las 18:32
[23] https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf Vistada 20/02/2019 a las 18:32
[24] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20180525 y https://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf Visitada 20/02/2019 a las 18:32
[25] https://www.riigiteataja.ee/akt/104012019011 Visitada 20/02/2019 a las 18:33
[26] https://www.finlex.fi/fi/laki/alkup/2018/20181050 Visitada 20/02/2019 a las 18:34
[27] http://www.parlament.hu/irom41/00335/00335.pdf Visitada 20/02/2019 a las 18:35
[28] http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html Visitada 20/02/2019 a las 18:35
[29] https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg Visitada 20/02/2019 a las 18:35
[30] https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums Visitada 20/02/2019 a las 18:35
[31] https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/952a77b0709011e8a76a9c274644efa9 Visitada 20/02/2019 a las 18:35
[32] http://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo Visitada 20/02/2019 a las 19:00
[33] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29098&l=1 Visitada 20/02/2019 a las 18:35
[34] https://zoek.officielebekendmakingen.nl/stb-2018-144.html Visitada 20/02/2019 a las 18:36

aprobada el 10 de mayo y entró en vigor el 25 de mayo de 2018[35] mientras que la segunda Ley está en fase de debate y se espera que sea aproba en el primer semestre de 2019; en Rumanía se promulgó la Ley 190/2018 que entró en vigor el 31 de julio de 2018[36]; Suecia por su parte aprobó la Ley de Protección de Datos 2018:218[37] legislación que entro en vigor el 25 de mayo de 2018 y; Reino Unido aprobó la "Data Protection Act"[38], la cual, entró en vigor el 25 de mayo de 2018.

En el caso de República Checa aún se está debatiendo en su cámara legislativa la Data Protection Act[39] que reemplazará a la ya existente Ley. Asimismo ocurre con Eslovenia cuya propuesta de Ley de Protección de Datos Personales (ZVOP-2)[40] fue presentada en enero de 2018, sin embargo, el Parlamento Esloveno fue disuelto para celebrar elecciones y hasta la fecha no se tienen más noticias sobre el proceso de aprobación de la meritada Ley; lo mismo ocurre con Grecia[41] que publicó su Proyecto de Ley el 20 de febrero de 2018 y desde entonces no se tienen noticias. Otro de los países que aún no se ha adaptado es Portugal, actualmente sigue en debate la Propuesta de Ley 120/XII[42], con lo cual, sigue vigente la Ley de Protección de Datos Personales 67/98 de 26 de octubre cuya última modificación fue con la Ley Nº. 103/2015 de 24 de agosto que fue la que incorporó a la legislación portuguesa la hoy derogada Directiva 94/46/EC[43].

[35] https://uodo.gov.pl/data/filemanager_pl/757.pdf Visitada 20/02/2019 a las 18:40

[36] https://iapp.org/media/pdf/resource_center/Romanian_Data_Protection_Law_English_Translation.pdf y https://www.senat.ro/legis/PDF/2018/18L294FP.pdf Visitada 20/02/2019 a las 18:50

[37] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218 Visitada 20/02/2019 a las 18:50

[38] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted Visitada 20/02/2019 a las 18:50

[39] http://www.psp.cz/sqw/historie.sqw?t=138&o=8 Visitada 20/02/2019 a las 18:50

[40] http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp.gov.si/novice/2018/ZVOP-2_NG_2_apr.pdf Visitada 20/02/2019 a las 18:35

[41] http://www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf Visitada 20/02/2019 a las 18:30

[42] http://debates.parlamento.pt/catalogo/r3/dar/s2a/13/03/089/2018-03-26/30?pgs=30-48&org=PLC Visitada 20/02/2019 a las 18:50

[43] https://wipolex.wipo.int/es/text/181654 Visitada 20/02/2019 a las 18:50

## 3. CONCLUSIONES Y DISCUSIÓN:

La protección de datos como tópico incardinado dentro de los Derechos Fundamentales, principalmente, dentro del Derecho a la intimidad y al honor, ha dejado hace mucho tiempo de ser una cuestión sobre la que apenas se hacían menciones, para convertirse en uno de los temas en el punto de mira a nivel mundial.

La adecuación al RGPD requiere de unos pasos internos y otros externos, los internos son: designar un Delegado de Protección de Datos; crear un Registro de actividades de tratamiento; realizar un análisis de riesgos; realizar una evaluación de impacto; estipular medidas ante posibles brechas de seguridad y; crear mecanismos y procedimiento de notificación a los usuarios y los externos son: la captación del consentimiento y Derechos de los usuarios, el estudio y la exhaustividad de los contratos de los encargados del tratamiento de datos y; la adaptación de la política de privacidad.

Después de la entrada en vigor y posterior obligatoriedad del RGPD, los países europeos se encuentran en fase de adaptación y adecuación normativa. A día de de hoy, es imposible saber el grado de adaptación en el que se encuentran debido a que sólo podremos saberlo en la medida en que se impongan sanciones, mientras que la adecuación normativa es mucho más sencilla de conocer. Hasta la fecha en su gran mayoría todos los Estados miembro han modificado sus respectivas legislaciones y en varios casos las han cambiado totalmente, reemplazando una por otra. Sin embargo, hay algunos países que siguen sin tener legislación adaptada al RGPD, cuestión que en teoría debería preocuparles, no obstante a nuestro modo de ver lo importante es que al menos dichos países ya tienen un proyecto de ley andando en sus respectivas cámaras legislativas.

## 4. REFERENCIAS:

*ÁLVAREZ HERNANDO,* J., Prácticum de Protección de Datos, Editorial Aranzadi, Madrid, 2018.

*RAMÍREZ DE MATOS,* E. *(Coord.);* Guía Rápida, Protección de Datos para Despachos de Abogados, Ilustre Colegio de Abogados de Madrid, Editorial Francis Lefebvre, Madrid, 2018.

**Webgrafía:**

- https://www.dlapiperdataprotection.com/index.html?t=about&c=GB Visitada 10/02/2019 las 18:00

-https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/ Visitada 10/02/2019 a las 19:00

**Legislación:**

*ZAKON O PROVEDBI OPĆE UREDBE O ZAŠTITI PODATAKA* (Ley de Protección de Datos de Croacia) https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html Visitada 20/02/2019 a las 18:33

*Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) ( Ley de Protección de Datos de Dinamarca) https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf Vistada 20/02/2019 a las 18:32*

*Законопроект за изменение и допълнение на Закона за защита на личните данни (Modificación de la Ley de Protección de Datos de Bulgaría ) https://www.parliament.bg/bg/laws/ID/78179 Visitada 20/02/2019 a las 18:30*

*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Francia) https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee Visitada 20/02/2019 a las 18:50*

*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y*

*garantía de los derechos digitales. https://iapp.org/media/pdf/resource_center/Spanish_data-protection-law.pdf Visitada 20/02/2019 a las 18:00*

*Ley 190/2018, de 26 de julio, de Protección de Datos (Rumanía) https://iapp.org/media/pdf/resource_center/Romanian_Data_Protection_Law_English_Translation.pdf y https://www.senat.ro/legis/PDF/2018/18L294FP.pdf Visitada 20/02/2019 a las 18:50*

*Isikuandmete kaitse seadus (Ley de Protección de Datos de Estonia) https://www.riigiteataja.ee/akt/104012019011 Visitada 20/02/2019 a las 18:40*

*Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. (Ley de Protección de Datos de Bélgica) https://iapp.org/media/pdf/resource_center/Belgian-GDPR-law_FR-DUTCH.pdf Visitada 20/02/2019 a las 18:30*

*"Bundesdatenschutzgesetz" (Ley de Protección de Datos Alemania) https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1553704155859 Visitada 20/02/2019 a las 18:51*

*Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG) (Ley de Protecciónd*

*de Datos Ausria) https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html Visitada 20/02/2019 a las 18:30*

*ΝΟΜΟΣ ΠΟΥ ΠΡΟΝΟΕΙ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΦΥΣΙΚΩΝ ΠΡΟΣΩΠΩΝ ΕΝΑΝΤΙ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΚΑΙ ΓΙΑ ΤΗΝ ΕΛΕΥΘΕΡΗ ΚΥΚΛΟΦΟΡΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΑΥΤΩΝ (Ley de Protección de Datos de Chipre)*

*http://www.cygazette.com/Gazette.dll/%7BA732F24B-2FD0-4D3D-884D-258C507E2509%7D/AppPgView?IssueNo=4670&PageNo=0&AppNo=1&PartNo=1&IssueDate=2/1/2013 Visitada 20/02/2019 a las 18:32*

Tietosuojalaki, Eduskunnan päätöksen mukaisesti säädetään: *(Ley de Protección de Datos de Finlandia) https://www.finlex.fi/fi/laki/alkup/2018/20181050 Visitada 20/02/2019 a las 18:35*

*2018. évi..... törvény* az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény jogharmonizációs célú módosításáról *(Ley de Protección de Datos de Hungría) http://www.parlament.hu/irom41/00335/00335.pdf Visitada 20/02/2019 a las 18:53*

DATA PROTECTION ACT 2018 *(Ley de Protección de Datos de Irlanda) https://data.oireachtas.ie/ie/oireachtas/act/2018/7/eng/enacted/a0718.pdf Visitada 20/02/2019 a las 18:53*

DECRETO LEGISLATIVO 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). *(Ley de Protección de Datos Italia) https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true Visitada 20/02/2019 a las 19:00*

Fizisko personu datu apstrādes likums *(Ley de Protección de Datos de Letonia) https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums Visitada 20/02/2019 a las 19:30*

LIETUVOS RESPUBLIKOS, ASMENS DUOMENŲ TEISINĖS APSAUGOS ĮSTATYMO NR. I-1374 PAKEITIMO ĮSTATYMAS *(Ley de Protección de Datos de Lituania) https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/952a77b0709011e8a76a9c274644efa9 Visitada 20/02/2019 a las 19:00*

Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État. *( Ley de Protección de Datos de Luxemburgo) http://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo Visitada 20/02/2019 a las 18:35*

Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations, 2018 *(Ley de Protección de Datos de Malta) http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29098&l=1 Visitada 20/02/2019 a las 17:00*

Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming) *(Ley de Protección de Datos de los Países Bajos) https://zoek.officielebekendmakingen.nl/stb-2018-144.html Visitada 20/02/2019 a las 14:00*

USTAWA, z dnia 10 maja 2018 r. o ochronie danych osobowych1 *(Ley de Protección de Datos Polaca) http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001000/O/D20181000.pdf Visitada 20/02/2019 a las 18:00*

Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Coll. *(Ley de Protecciónde Datos de Eslovaquia) https://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf Visitada 20/02/2019 a las 18:24*

Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning *(Ley de Protección de Datos de Suecia) http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2018219-med-kompletterande_sfs-2018-219 Visitada 20/02/2019 a las 18:30*

Data Protection Act 2018 *(Ley de Protección de Datos de Reino Unido) http://www.legislation.gov.uk/ukpga/2018/12/introduction/enacted Visitada 20/02/2019 a las 19:30*

*Proyectos de Ley:*

*PŘEDKLADATEL, Vláda předložila sněmovně návrh zákona 28. 3. 2018.*

*Zástupce navrhovatele: ministr vnitra. (Proyecto de Ley de Protección de Datos de República Checa) http://www.psp.cz/sqw/historie.sqw?o=8&t=138 Visitada 20/02/2019 a las 19:30*

*Predlog Zakona o varstvu osebnih podatkov – predlog za obravnavo – nujni postopek–NOVO GRADIVO ŠT.2 (Proyecto de Ley de Protección de Datos de Eslovenia) http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp.gov.si/novice/2018/ZVOP-2_NG_2_apr.pdf Visitada 20/02/2019 a las 18:30*

*Νόμοσ για την Προςταςύα Δεδομϋνων Προςωπικού Φαρακτόρα (Proyecto de Ley de Protección de Datos de Grecia) http://www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf Visitada 20/02/2019 a las 19:30*

*PROPOSTA DE LEI N.º 120/XIII (3.ª)ASSEGURA A EXECUÇÃO, NA ORDEM JURÍDICA NACIONAL, DO REGULAMENTO (UE) 2016/679, RELATIVO À PROTEÇÃO DAS PESSOAS SINGULARES NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS E À LIVRE CIRCULAÇÃO DESSES DADOS (Propuesta de Proyecto de Ley de Protección de Datos Portugal) http://debates.parlamento.pt/catalogo/r3/dar/s2a/13/03/089/2018-03-26/30?pgs=30-48&org=PLC Visitada 20/02/2019 a las 19:00*